航天产品共因失效分析流程

中国航天科技集团公司可靠性与安全性研究中心 刘春雷 任立明

摘 要 主要针对共因失效产生的原因及共因失效分析的开展时机、实施流程、跟踪报告表格格式等做了说明，为在航天型号内开展共因失效分析提供了指导。

关键词 航天产品 可靠性 安全性 共因失效

一、概述

当前，长寿命高可靠已经成为航天器研制所必须考虑的重要内容，而采用冗余技术是提高产品可靠性的有效途径[1]。冗余技术指的是通过投入超过常规设计所需的外加资源，抵消故障产生的后果，达到提高可靠性的目的（外加资源一般包括硬件、信息、时间和软件等）。

共因失效是冗余系统提前失效的重要原因之一。共因失效指的是两个或多个部件在同一时间或在相对很短间隔内由于共同原因所导致的失效。共因失效是各类系统中广泛存在的一种相关失效形式，这种失效形式的存在严重影响了冗余系统的安全性和可靠性。从核电厂及美国航天飞机的概率安全评估中可以看到，由共因造成的多元件失效是核电厂及航天飞机系统中的冗余系统失效的主要因素之一，因此，许多国家在一些复杂系统的可靠性研究中都要求进行共因失效分析[3]。

当一个冗余系统由相同部件、位置或方法组成时，发生共因失效的可能性就会大大增加。以下例子均为由于共因失效所导致的失效或事故[3]：

1）STS-9 中的胼泄漏导致两个 APU 爆炸；

2）飞行器的多引擎失效（Fokker F27-1997，1988；Boeing 747，1992）；

3）1989 年 DC-10 由于 2# 引擎失效导致的液压系统失效；

4）三哩岛 NPP 的三台辅助给水泵同时失效；

5）51L 航天飞机上的固体推进器由于两个 O 形环失效导致的高温气体泄漏。

二、方法研究

1. 共因失效产生原因

共因失效通常被认为是由以下两个原因造成的：一是根本性原因，即共因失效事件中导致每个部件都失效的共性原因；另一个是指导致并联部件同时失效的耦合原因。举例来说，两个完全相同的冗余电气元件由于暴露在过高的温度下导致失效的原因不仅是由于元件对热的敏感性（根本性原因），而且还由于两个元器件是完全相同的并且同时暴露在了相同恶劣的环境下导致的（耦合因素）。

近几年，人们对系统失效的相关性有了更深刻的认识。目前人们已经认识到相关失效是系统失效的基本特征，而独立失效只是一种很特殊的情况。相关关系可以根据是由系统的已知功能和物理特性产生的还是由于外部因素或不确定性产生的进行分类，一般可以分为系统内在或者外在两种。

同时，人们也认识到，通常很多失效都发生在部件间的连接处，或者是各分系统以及系统之间的接口部分，其中还包括一个很重要因素——环境因素[4]。当系统设计时的某一部分与另一部分相关，或者两个部分之间有相互作用或具有相同的环境时，那么就有发生共因失效的危险。一般，由相关事件引起的失效通常很难鉴别，但是如果在分析中不考虑这一因素就会导致对事故风险的错误低估。大量经验表明，检查所有的共因或共同事件是可以做到的[8]。这些主要用来处理物理位置和制造特

性，例如：所处的共同环境、通过共同插座或插头连接的导线、导致相同初始缺陷的相同的设计流程、在安装和维护过程中可能由于采用有缺陷设备或流程导致的校正错误等。

2. 共因失效分析流程概述

共因失效分析可以分以四个步骤进行：

1）建立系统逻辑模型

这个阶段要求对系统有个基本的认识，一般需要考虑故障模式、边界条件和逻辑模型等。

2）识别共因事件组

对所有可能发生共因失效的系统单元进行检查，以发现根本原因和耦合因素并确定进一步共因失效建模的优先次序。

3）共因建模和数据分析

这个阶段主要利用经验数据选择所要使用的共因失效模型、最小割集和参数估计等。

4）系统量化和结果的进一步解释

这个阶段确定系统失效的可能性和共因失效对最终结果的影响，主要包括敏感性分析和备选后续措施的选择等。

3. 共因失效分析开展时机

功能级的共因失效分析应该在项目论证阶段开始实施，目的是识别设计过程中的关键项目。详细的或部件级的共因失效分析只有在详细设计完成之后才能开展。

具体共因失效分析工作应该在建立详细的系统故障树以及开始识别最小割集的时候开始实施。选择这些最小割集的原因是因为它们包含可能由于配置、环境因素、共同工艺等共同因素或环境等原因导致失效的关键部件。这些关键部件可以通过FMEA来识别。利用FMEA识别共因失效的具体流程参见图1。

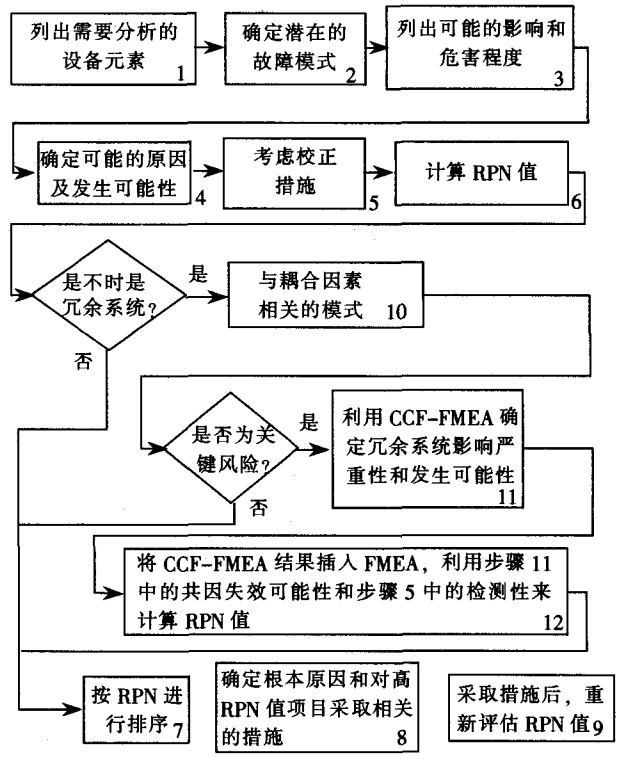

图 1　利用 FMEA 识别共因失效流程

三、定性共因失效分析程序

定性共因失效分析的分析过程可以分为三步并使用3~4张检查单来完成。第一张检查单用来检查一部分相互关联或冗余的部件来识别共同性。这个共性检查单可以针对具体项目、使用限制或经验等进行修改，共性检查单如表1所示。第二张检查单主要用来针对以上步骤中识别出来的共性在共性领域内检查可能出现的关键状态，检查单如表2所示。第三张检查单用来指出可能发生的事故的激发事件、机理或原因，检查单如表3所示。这里需要指出的是，并不是某一关键故障的所有可能原因都要预先决定。如果单一原因就可以导致关键事故就不需要考虑所有其它相关的事件。纠正措施通常可用来降低由于任何诱发事件引起的所有类别的状态的设计敏感性。因此，第三张检查单代表了对可能的激发事件情况的研究。

表 1　共性检查单

类别	具体内容
位置和环境	机箱、包装、外壳、高度（上升）
设计与制造	设计、零件号码、设备名称或条款、流程、校正、试验、系统/部件接口
维护	周期、校正设备、人员、材料
操作	特性展示、输入

表 2　关键状态检查单

类别	具体内容
电	短路、断路、振荡
机械	分离、冲击焊接、堵塞
化学、腐蚀	
生物	

表 3 事故的激发事件、机理或原因检查单

类别	具体内容
可能的事故的激发事件、机理或原因	导电物的污染
	机械剪切
	火、爆炸
	洪 水
	降温失败
	灰 尘 等

必须对每种重要的活动都进行记录，否则每种分析工作都没有达到预期目的。应该对所得到的结论或结果进行及时的记录，并且通过恰当的决策来进行追踪，不然，一些重要方面就可能被忽视或者所采用的校正措施不但不能起到校正的作用，反而可能会导致更坏的结果。任何种类的追踪格式都可以用来记录所做工作的覆盖程度，但是重要危险及相关预期事故一般应该单独报告、阐述、编号，并且按照高风险项目进行追踪。定性共因失效分析流程如图 2 所示。工作主要分四个步骤：

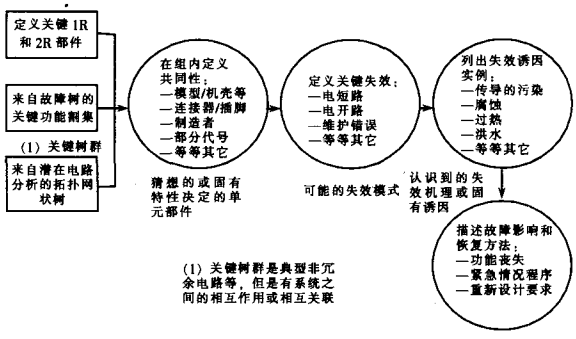

图 2 定性共因失效分析步骤

首先，识别并列出所有树或部件之间的共性。这些共性可能是共用的连接器，就舱内、机壳、线束等来说的相同位置，或其它更加一般的特性，如相同厂家或其它特性。第二个步骤是确定可以想到的每个树或部件内的失效模式或所有单元部件。举例说明失效模式如：电的短路和开路，维护错误或校正的错误。第三步是要求记录至少一个在第二步中识别出来失效模式的可能的原因。

试图列出所有这些失效模式下的可能原因是不可能的，但是列出至少一个可能的初始事件用来说明需要改进设计就已经足够了，并且任何修改后的设计应该消除对相似原因的功能敏感性。全面的风险评价结果可能相对于每种推荐的特有诱因机制而变化很大。在第三步列出的原因包括：导电物的污染、机械切割、着火、爆炸、洪水等或其它能够导致电短路、断路、维修错误等的其它机制。定性共因失效分析程序的最后一步是描述在第二步骤中列出的条款下的失效的影响以及恢复方法。这些内容应该记录成方便以后追踪、风险评估或解决的形式，如表 4 所示。

表 4 定性共因失效分析追踪和解决表格

关键功能集	共性	关键事件	潜在原因	影响	备注

四、共因失效量化分析

定性分析得到了所有可能造成共因失效的系统缺陷。采用定性分析可以大大减小分析问题的范围，但是对所有的共因缺陷进行详细建模和分析工作量太大，仍然无法进行，而且也超出了分析者所掌握的资料和能力范围。因此接下来就需要继续缩小问题的范围，从而能够更详细的分析共因系统的关键缺陷。我们可以通过定量筛选分析来缩小范围。

在进行定量共因失效分析时，只要我们选用的不是一个保守的而且已经经过简化的模型，我们就需要进行进一步详细的定量分析。量化分析可以参考以下步骤：

1）我们通过改变部件级的故障树来明确共因部件组中的每个部件可能的“全局”或“最大”的共因失效事件。一组部件的全局共因事件是指组内的所有单元都失效。最大共因事件是指代表两个或更多共因的基本事件。举例来说明，我们考虑由部件 A，B，C 组成的共因部件组，根据规则故障树的基本事件包括：“A 失效”、“B 失效”或“C 失效”，扩展的基本事件 C_{ABC} 指 A、B、C 同时失效，如图 3 所示：

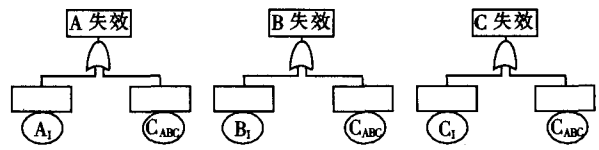

图 3 扩展 A、B、C 失效模型

2）这里 A_I、B_I、C_I 分别表示部件 A、B、C 的独立失效。相应的分别代表故障树中的基本事件“A 失效”、“B 失效”或“C 失效”。

3）我们通过解故障树来得到系统或者事故序列的最小割集。其中每个包含交集 $A_IB_IC_I$ 的割集都含有 C_{ABC}。这一步骤的意义在于在复杂系统模型或事件序列中，基于发生概率的割集的取舍过程中必须从根本上获得解决，由于独立失效 $A_IB_IC_I$ 的值太小通常在取舍最小割集的过程中都被忽略了，而共因项 C_{ABC}（数值较大）就可以保留下来。

4）共因基本事件的值可以通过一个简单的全局参数模型来估计 [4]：

$$P_r(C_{ABC}) = gP_r(A)$$

$P_r(A)$ 是部件的失效概率。g 的值一般取在 0.05 到 0.10 之间，如果要得到更精确的值的话应根据不同配置（n 取 k 模型）进行考虑。表 5 列出了 n 取 k 模型系统配置中全局共因因子 g 的值，具体取值方法见参考文献 [6]。不同的 g 值是根据部件是同时检测（不交叉）得到的还是在固定时间间隔（交叉）内分别检测得到的。原因及更多细节参考文献 [7]。

这种简单的全局或最大参数模型对共因失效发生频率做了一个保守估计，而不考虑共因部件组中的冗余部件数量。

那些对系统失效或事件序列的频率作用不大（或按发生概率太小取舍时未作保留）的共因部件组将不在进一步的分析中予以考虑。那些对系统失效或事件序列频率作用巨大的共因部件组保留下来，进行进一步定性和定量分析。

表 5 不同系统配置全局共因因子（g）的筛选值

有效配置	g 值	
	交叉检测	不交叉检测
2 取 1	0.05	0.10
2 取 2		
3 取 1	0.03	0.08
3 取 2	0.07	0.14
3 取 3		
4 取 1	0.02	0.07
4 取 2	0.04	0.11
4 取 3	0.08	0.19
4 取 4		

不论定性分析还是定量分析的目的都是确定潜在的共因缺陷，并找出那些对系统失效作用不大的以不对它们进行详细分析。如果我们能够接受保守估计并且已经达到了研究目的，那么分析就可以到此为止。否则在筛选分析中保留下来的部件组还需要进一步详细的建模分析。

五、结语

冗余技术是当前提高航天系统可靠性、安全性的重要途径，而共因失效是导致冗余系统提前失效的重要原因。本文对共因失效产生的原因及共因失效分析的开展时机、实施过程、跟踪报告格式均做了说明，为在航天型号内广泛开展共因失效分析提供了理论及技术上的支持。

参考文献

[1] 孙凝生. 冗余设计技术在运载火箭飞行控制系统中的应用(一) [J]. 航天控制,2003.

[2] Collas G. Reliability engineering for the future, In: New trends in system reliability evaluation, K. B. Misra(ed.),El-sevier,325-328, 1993.

[3] NASA《Probabilistic Risk Assessment Procedures Guide for NASA Managers and Parishioners》, 2002.

[4] Dore P. Basic aspects of stochastic reliability analysis for redundancy systems [j]. Reliability Eng, &System Safety, 24; 351-375,1987.

[5] A.Mosleh, et al, “Procedures for Treating Common Cause Failures in Safety and Reliability Studies,” U.S.Nuclear Regulatory Commission and Electric Power Research Institute, NUREG/CR-4780, and EPRI NP-5613.Volumes 1 and 2,1988.

[6] NSTS 22254《Methodology for Conduct of Space Shuttle Program Hazard Analyses》,2004.

[7] NASA 《Fault Tree Handbook with Aerospace Applications》,2002.

[8] Gaspare Maggio.Space Shuttle Probabilistic Risk Assessment: Methodology & Application. NASA. 1996.